CONSTRUCTING HYPERELLIPTIC CURVES WITH SURJECTIVE GALOIS REPRESENTATIONS

SAMUELE ANNI AND VLADIMIR DOKCHITSER

Abstract. In this paper we show how to explicitly write down equations of hyperelliptic curves over $\mathbb{Q}$ such that for all odd primes ℓ the image of the mod ℓ Galois representation is the general symplectic group. The proof relies on understanding the action of inertia groups on the ℓ-torsion of the Jacobian, including at primes where the Jacobian has non-semistable reduction. We also give a framework for systematically dealing with primitivity of symplectic mod ℓ Galois representations.

The main result of the paper is the following. Suppose $n = 2g + 2$ is an even integer that can be written as a sum of two primes in two different ways, with none of the primes being the largest primes less than n (this hypothesis is expected to hold for all $g \neq 0, 1, 2, 3, 4, 5, 7$ and 13). Then there is an explicit $N \in \mathbb{Z}$ and an explicit monic polynomial $f_0(x) \in \mathbb{Z}[x]$ of degree n, such that the Jacobian J of every curve of the form $y^2 = f(x)$ has $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for all odd primes ℓ and $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q}) \cong S_{2g+2}$, whenever $f(x) \in \mathbb{Z}[x]$ is monic with $f(x) \equiv f_0(x) \bmod N$ and with no roots of multiplicity greater than 2 in $\overline{\mathbb{F}}_p$ for any $p \nmid N$.

Contents

2010 *Mathematics Subject Classification.* Primary 11F80, Secondary 12F12, 11G10, 11G30.

Key words and phrases. Galois representations, abelian varieties, hyperelliptic curves, inverse Galois problem, Goldbach's conjecture.

1. Introduction

A classical method for showing that the group $\mathrm{GL}_2(\mathbb{F}_\ell)$ is a Galois group over $\mathbb{Q}$ is by realising it as the Galois group of the field generated by the ℓ-torsion on an elliptic curve. One can similarly try to construct the general symplectic group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as the Galois group associated to the ℓ-torsion of a g-dimensional abelian variety. The main difficulty is that it is much harder to write down explicit abelian varieties and then verify that the Galois group obtained is not a proper subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. This approach has been successfully used in a number of works, including [Zar79], [SZ05], [Hal08], [Zar10], [Hal11], [AV11], [AK13], [AAK$^+$15], which realise $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for every (odd) prime ℓ using Jacobians of hyperelliptic curves, and show that one curve often realises $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for all sufficiently large ℓ. More recently [LSTX19] gave a non-constructive proof that many hyperelliptic curves realise $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for all odd primes ℓ, and [Die02], [Zyw15], [ALS16] who exhibited explicit curves of genus 2 and 3 with this property. There has also been numerical work [AAK$^+$16], [ALS16] investigating the Galois images of Jacobians of curves, and work on general abelian varieties [Lom15].

The main contribution of the present article to this topic is an explicit construction of hyperelliptic curves, such that for every prime ℓ their Jacobian has maximal mod ℓ Galois image; in other words hyperelliptic curves whose Jacobian J has $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for every odd prime ℓ, and isomorphic to the symmetric group S_{2g+2} for $\ell = 2$.

The key new tool is a way of controlling the action of inertia groups on $J[\ell]$ at places where J has non-semistable reduction. Our approach does, however, require a rather unorthodox constraint on the dimension g: we need the even integer $2g + 2$ to satisfy Goldbach's conjecture. In fact, we require it to satisfy the following somewhat stronger statement, which appears to hold[1] for every genus $g \neq 0, 1, 2, 3, 4, 5, 7, 13$:

Conjecture (Double Goldbach)**.** *Every positive even integer n can be written as a sum of two primes in two different ways with none of the primes being the largest prime less than n, except for $n = 0, 2, 4, 6, 8, 10, 12, 16, 28$.*

The result on Galois images of hyperelliptic curves that we obtain is the following:

Theorem 1.1. *Let g be a positive integer such that $2g + 2 = q_1 + q_2 = q_4 + q_5$ for some primes q_i, with $\{q_1, q_2\} \neq \{q_4, q_5\}$, and that there is a further prime q_3 with $q_1, q_2, q_4, q_5 < q_3 < 2g + 2$. Then there exist an explicit $N \in \mathbb{Z}$ and an explicit $f_0 \in \mathbb{Z}[x]$ monic of degree $2g + 2$ such that if $f(x) \in \mathbb{Z}[x]$ satisfies:*

(1) $f(x) \equiv f_0 \bmod N$, and
(2) $f(x) \bmod p$ has no roots of multiplicity greater than 2 for all primes $p \nmid N$,

then $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \text{ for all primes } \ell \neq 2, \\ S_{2g+2} \text{ for } \ell = 2, \end{cases}$ *where* $J = \mathrm{Jac}(y^2 = f(x))$.

[1] We have made a quick numerical check: the property holds for all other $g < 10^7$.

See Theorem 7.1 for the explicit description of N and $f_0(x)$, and Remark 7.2 for an explanation on how to find explicit curves satisfying hypothesis (2). An explicit example for $g = 6$ is given in Section 8.

For the exceptional genera $g = 1, 2, 3, 4, 5, 7, 13$ our method still makes it possible to construct hyperelliptic curves with maximal image at all but a small number of primes, e.g. all primes except $\ell = 5, 11, 13$ when $g = 7$ (see Remark 6.6).

It is worth noting that hypotheses (1) and (2) in the above theorem are satisfied by a positive density of monic polynomials $f(x)$, for example see [BSW16, Theorem 1.5]. In particular, this shows that the hyperelliptic curves of genus g with maximal mod ℓ Galois image for every prime ℓ have a positive (lower) density among all hyperelliptic curves of genus g.

Throughout the paper we work with hyperelliptic curves

$$C : y^2 = f(x)$$

and write

$$J = \mathrm{Jac}(C)$$

for their Jacobian. The layout is as follows.

In Section 2 we examine the Galois representations $H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)$ and $J[\ell]$ as representations of local Galois groups. For the "$\ell \neq p$" theory we use the method of clusters, recently introduced in [DDMM18]. For "$\ell = p$" we restrict our attention to primes p of semistable reduction, and use the description given by the theory of fundamental characters. We also give a simple criterion guaranteeing that a local Galois group contains a transvection in its action on $J[\ell]$.

In Section 3 we develop criteria for the representations $H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)$ and $J[\ell]$ to be globally irreducible. This is the place where the "double Goldbach" hypothesis enters. The reason for it is that we cannot always guarantee that the above representations are locally irreducible. In fact, this appears to be a genuine obstruction: for example, there is no 17-dimensional abelian variety $A/\mathbb{Q}_p$ and primes $p > 35$ and $\ell \neq p$, such that $T_\ell(A) \otimes \overline{\mathbb{Q}}_\ell$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module[2]. However, when $2g + 2$ is a sum of two primes (other than ℓ), we are able to force the local representation to have at most two irreducible constituents. To guarantee global irreducibility we then use conditions of this kind at several places. The reason that we require "double Goldbach" rather than the classical Goldbach's conjecture, is so that we can treat the case when ℓ is one of the Goldbach prime summands of $2g + 2$ by using the other pair of primes.

In Section 4 we develop criteria for the representations $H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)$ and $J[\ell]$ to be primitive. The basic method essentially follows that of Serre (see e.g. [Maz78, Theorem 4] or [AS15, §1]) or, more recently [ALS16]: we ensure that every inertia group acts trivially on every possible Galois stable partition of the representation and then invoke the Hermite-Minkowski theorem to deduce that no such partition exists. We formalise this approach by introducing "quasi-unramified" representations, and develop the necessary conditions on $f(x)$ that make the argument work

[2]The hypotheses ensure that A has potentially good reduction and the inertia group at p acts tamely and semisimply on $T_\ell(A)$, through a cyclic quotient of order k, say. Any element of the inertia group must have rational trace on $T_\ell(A)$ (as the trace is independent of ℓ), so irreducibility forces the eigenvalues of a generator of the image of inertia to be precisely the set of k-th roots of unity. Hence $34 = \dim T_\ell(A) \otimes \overline{\mathbb{Q}}_\ell = \varphi(k)$, which is impossible.

("admissible" and "p-admissible" polynomials). Unlike [ALS16], it is important for us to allow for curves with non-semistable reduction.

In Section 5 we recall the classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of [Hal08] and [ADW16] and rephrase it as a criterion for J to have $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. As in many previous works, the basic rule is that if the action is irreducible, primitive and contains a transvection, then the Galois representation has maximal image (see Theorem 5.1).

In Section 6 we tie everything together to give a list of (essentially local) constraints that guarantee that $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for every odd prime ℓ, and that $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q}) \cong S_{2g+2}$; see Theorems 6.2 and 6.5.

In Section 7 we give explicit congruence conditions on the coefficients of $f(x)$ that ensure that the above list of constraints is satisfied, and prove the precise version of Theorem 1.1 (see Theorem 7.1).

We end in Section 8 by working through the conditions in Theorem 7.1 for $g = 6$, and constructing a hyperelliptic curve satisfying all the hypotheses.

Acknowledgments. We would like to thank Adam Morgan and Tim Dokchitser for several useful discussions related to this work and the referee for their comments. The first author was supported by EPSRC Programme Grant 'LMF: L-Functions and Modular Forms' EP/K034383/1 during his position at the University of Warwick, and by DFG Priority Program SPP 1489 and the Luxembourg FNR during his positions at IWR, Heidelberg and at the University of Luxembourg. The second author is supported by a Royal Society University Research Fellowship. Both authors would also like to thank the Warwick Mathematics Institute where most of this research was carried.

1.1. Notation, t-Eisenstein polynomials and type $t - \{q_1, \ldots, q_k\}$.

Local setting. For a finite extension F of $\mathbb{Q}_p$ we write:

- π_F for a fixed uniformizer of F;
- $\mathcal{O}_F$ for the ring of integers of F;
- e_F for the ramification degree of F;
- $\overline{F}$ for a fixed algebraic closure of F;
- F^{nr} for the maximal unramified extension of F;
- v for a valuation on $\overline{F}$ normalized such that $v(\pi_F) = 1$;
- $\mathbb{F}$ for the residue field of F;
- G_F for the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$;
- I_F for the inertia subgroup of G_F;
- $\overline{g}(x)$ and $\overline{\alpha}$ for the reduction modulo π of every $g(x) \in \mathcal{O}_F[x]$ and $\alpha \in \mathcal{O}_F$.

Definition 1.2 (t-Eisenstein polynomials)**.** Let $t \geq 1$ be an integer. We say that a polynomial with $\mathcal{O}_F$-coefficients

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

is *t-Eisenstein* if $v(a_i) \geq t$ for all $i > 0$ and $v(a_0) = t$.

Definition 1.3 (Polynomials of type $t-\{q_1,\ldots,q_k\}$)**.** Let $q_1,\ldots,q_k$ be prime numbers and let $t\geq 1$ be an integer. Let $f(x)\in\mathcal{O}_F[x]$ be a monic squarefree polynomial. We say that $f(x)$ is of *type* $t-\{q_1,\ldots,q_k\}$ if it can be factored as

$$f(x)=h(x)\prod_{i=1}^{k}g_i(x-\alpha_i)$$

over $\mathcal{O}_F[x]$, for some $\alpha_i\in\mathcal{O}_F$ with $\overline{\alpha}_i\neq\overline{\alpha}_j$ for all $i\neq j$, where $g_i(x)$ is a t-Eisenstein polynomial of degree q_i and $\overline{h}(x)$ is separable with $\overline{h(\alpha_i)}\neq 0$ for all i.

In other words, the monic polynomial $f(x)$ is a product of shifted t-Eisenstein polynomials of degrees $q_i,\ldots q_k$ and linear polynomials, such that these polynomials have no common roots in the residue field. See Section 8 for explicit examples.

Global setting. For a number field K we write:

- $\mathcal{O}_K$ for the ring of integers of K;
- $\mathbb{F}_{\mathfrak{p}}$ for the residue field of K at a prime $\mathfrak{p}$ of K;
- $\overline{K}$ for a fixed algebraic closure of K;
- G_K for the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$;
- $I_{\mathfrak{p}}=I_{K_{\mathfrak{p}}}$ for the inertia subgroup at $\mathfrak{p}$.

Definition 1.4. Let $q_1,\ldots,q_k$ be prime numbers. Let $f(x)\in\mathcal{O}_K[x]$ be a monic squarefree polynomial. We say that f is of *type* $t-\{q_1,\ldots,q_k\}$ at $\mathfrak{p}$ if $f(x)\in\mathcal{O}_{K_{\mathfrak{p}}}[x]$ is of type $t-\{q_1,\ldots,q_k\}$.

Roots of unity. Let q be a positive integer, we will denote by ζ_q a primitive q-th root of unity. Throughout this article we will choose primitive roots of unity to form compatible systems, i.e. if ζ_q is a primitive q-th root of unity and $q=q'q''$ then $\zeta_q^{q''}=\zeta_{q'}$. In characteristic ℓ dividing q, we have $\zeta_q=\zeta_m$ where $\ell^r m=q$, with $(\ell,m)=1$.

2. Inertia action on $J[\ell]$

The construction of hyperelliptic curves presented in this article will crucially rely on understanding the action of the inertia groups on the ℓ-torsion of the Jacobian for every prime number ℓ. In this section, F will be a local field of odd residue characteristic p. Let

$$C: y^2=f(x)$$

be a genus g hyperelliptic curve over F with $f(x)\in\mathcal{O}_F[x]$ monic and squarefree, and let $J=\mathrm{Jac}(C)$. We will describe the inertia action on $J[\ell]$ in terms of $f(x)$.

2.1. $J[\ell]$ when $\ell\neq p$: clusters.

In this section we describe the inertia action on $J[\ell]$ when $\ell\neq p$. In particular, we will prove the following theorem:

Theorem 2.1. *Suppose that $f(x)\in\mathcal{O}_F[x]$ has type $t-\{q_1,\ldots,q_k\}$ for odd primes $q_i\neq p$. Then for every $\ell\neq p$, the inertia group I_F acts tamely on $H^1_{\acute{e}t}(C/\overline{F},\mathbb{Q}_\ell)$ and on $J[\ell]$ through a quotient of order dividing $2\prod_i q_i$. Moreover, the non-trivial eigenvalues (with multiplicity) of any generator τ of tame inertia are either*

$$-\zeta_{q_1},-\zeta_{q_1}^2,\ldots,-\zeta_{q_1}^{q_1-1},\ldots,-\zeta_{q_k},-\zeta_{q_k}^2,\ldots,-\zeta_{q_k}^{q_k-1}\quad \textit{if } t \textit{ is odd,}$$

or

$$\zeta_{q_1},\zeta_{q_1}^2,\ldots,\zeta_{q_1}^{q_1-1},\ldots,\zeta_{q_k},\zeta_{q_k}^2,\ldots,\zeta_{q_k}^{q_k-1}\quad \textit{if } t \textit{ is even.}$$

The main ingredient of the proof of Theorem 2.1 is the theory of clusters developed in [DDMM18].

Definition 2.2. Let $f(x) \in \mathcal{O}_F[x]$ be a squarefree monic polynomial and let R be its set of roots in $\overline{F}$. A *cluster* $\mathfrak{s} \subseteq R$ is a non-empty set of roots of $f(x)$ of the form $\mathfrak{s} = R \cap \mathcal{D}$ for a disc $\mathcal{D} \subseteq \overline{F}$ with respect to the p-adic topology.

For a cluster $\mathfrak{s}$ with $|\mathfrak{s}| \geq 2$ define:

- $d_{\mathfrak{s}} = \min\{v(r-r') : r, r' \in \mathfrak{s}\}$;
- $\mathfrak{s}_0$ to be the set of maximal subclusters of $\mathfrak{s}$ of odd size;
- $I_{\mathfrak{s}} = \mathrm{Stab}_{I_F}(\mathfrak{s})$, the stabiliser of $\mathfrak{s}$ in $I_{\mathfrak{s}}$;
- $\mu_{\mathfrak{s}} = \sum_{r \in R \setminus \mathfrak{s}} v(r - r_0)$ for any $r_0 \in \mathfrak{s}$;
- $\lambda_{\mathfrak{s}} = \frac{1}{2}(\mu_{\mathfrak{s}} + d_{\mathfrak{s}}|\mathfrak{s}_0|)$;
- $\epsilon_{\mathfrak{s}} = \begin{cases} \text{trivial character } \mathbf{1} \text{ of } I_{\mathfrak{s}} & \text{if } |\mathfrak{s}| \text{ is even and } \mathrm{ord}_2(\mu_{\mathfrak{s}} \cdot |I_F/I_{\mathfrak{s}}|) \geq 1 \\ \text{order two character of } I_{\mathfrak{s}} & \text{if } |\mathfrak{s}| \text{ is even and } \mathrm{ord}_2(\mu_{\mathfrak{s}} \cdot |I_F/I_{\mathfrak{s}}|) < 1 \\ \text{zero representation of } I_{\mathfrak{s}} & \text{otherwise ;} \end{cases}$
- $\gamma_{\mathfrak{s}} : I_{\mathfrak{s}} \to \mathbb{C}^*$ any character of order equal to the prime-to-p-part of the denominator of $|I_F/I_{\mathfrak{s}}| \cdot \lambda_{\mathfrak{s}}$ (with $\gamma_{\mathfrak{s}} = \mathbf{1}$ if $\lambda_{\mathfrak{s}} = 0$);
- $V_{\mathfrak{s}} = \gamma_{\mathfrak{s}} \otimes (\mathbb{C}[\mathfrak{s}_0] \ominus \mathbf{1}) \ominus \epsilon_{\mathfrak{s}}$, an $I_{\mathfrak{s}}$-representation. (We write $\ominus$ for the "direct difference" of representations, that is $A \ominus B = C$ if and only if $B \oplus C = A$).

Theorem 2.3 ([DDMM18, Theorem 1.19])**.** *Let ℓ be a prime different from p, then*

$$H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell) \cong H^1_{ab} \oplus (H^1_t \otimes \mathrm{Sp}(2))$$

as I_F-representations, with

$$H^1_{ab} = \bigoplus_{\mathfrak{s} \in X/I_F} \mathrm{Ind}_{I_{\mathfrak{s}}}^{I_F} V_{\mathfrak{s}}, \qquad H^1_t = \bigoplus_{\mathfrak{s} \in X/I_F} (\mathrm{Ind}_{I_{\mathfrak{s}}}^{I_F} \epsilon_{\mathfrak{s}}) \ominus \epsilon_R,$$

where X is the set of clusters that are neither singletons nor (proper) disjoint unions of even size clusters, X/I_F is a set of I_F-orbit representatives, and where $\mathrm{Sp}(2)$ *denotes the 2-dimensional special ℓ-adic representation.*[3]

Remark 2.4. When J is semistable we will refer to the dimension of H^1_t as the toric dimension of J. If the dimension of H^1_t is equal to the genus g, we say that the reduction is totally toric.

Lemma 2.5. *Let $f(x) \in \mathcal{O}_F[x]$ be a t-Eisenstein polynomial of degree n, with $(n, tp) = 1$. Then I_F acts tamely on the roots of $f(x)$ and permutes them cyclically and transitively. Moreover, $v(r - r') = \frac{t}{n}$ for any two roots $r \neq r'$ of $f(x)$.*

Proof. Let r be a root of $f(x)$. The Newton polygon of $f(x)$ has a unique slope equal to $-\frac{t}{n}$, so all the roots of $f(x)$ have valuation $\frac{t}{n}$. In particular, $f(x)$ is irreducible and the field $F^{\mathrm{nr}}(r)$ is a tamely ramified extension of degree n of F^{nr}. By uniqueness, it is Galois and its Galois group is C_n. As $f(x)$ is irreducible over F^{nr}, the cyclic group C_n acts transitively on the roots of $f(x)$.

[3] Let ℓ and p be distinct prime numbers. The *special representation* $\mathrm{Sp}(2)$ over a local field $F/\mathbb{Q}_p$ is the (tame) 2-dimensional ℓ-adic representation given by:

$$\mathrm{Sp}(2)(\tau) = \begin{pmatrix} 1 & t_\ell(\tau) \\ 0 & 1 \end{pmatrix}, \quad \mathrm{Sp}(2)(\mathrm{Frob}_{\overline{F}/F}) = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{q} \end{pmatrix},$$

where $\tau \in I_F$, the character $t_\ell(\tau)$ is an ℓ-adic tame character, $\mathrm{Frob}_{\overline{F}/F}$ is a fixed Frobenius element and $q = \#\mathbb{F}$.

Since the extension $F^{\mathrm{nr}}(r)/F^{\mathrm{nr}}$ is tame, the standard homomorphism

$$\mathrm{Gal}(F^{\mathrm{nr}}(r)/F^{\mathrm{nr}}) \to \overline{\mathbb{F}}^*; \qquad \sigma \mapsto \frac{\sigma(r)}{r}$$

is injective. In particular if σ is non-trivial then $\frac{\sigma(r)}{r} \neq 0, 1$ in $\overline{\mathbb{F}}$, and hence $v(\sigma(r) - r) = v(r) = \frac{t}{n}$. As I_F acts transitively on the roots, this shows that $v(r - r') = \frac{t}{n}$ for any distinct pair of roots r, r' of $f(x)$. □

Lemma 2.6. *Suppose that $f(x) \in \mathcal{O}_F[x]$ has type $t - \{q_1, \ldots, q_k\}$ with $(q_i, tp) = 1$ for all i and let $f(x) = h(x) \prod_{i=1}^{k} g_i(x - \alpha_i)$ be the corresponding factorisation as in Definition 1.3. Let $\beta_{i,1}, \ldots, \beta_{i,q_i}$ be the roots of $g_i(x - \alpha_i)$ and let $\beta_{0,1}, \ldots, \beta_{0,\deg h}$ be the roots of $h(x)$.*

(i) If $i \neq j$, then $v(\beta_{i,a} - \beta_{j,b}) = 0$ for all a, b.
(ii) If $i \neq 0$, then $v(\beta_{i,a} - \beta_{i,b}) = \frac{t}{q_i}$ for all $a \neq b$.
(iii) $v(\beta_{0,a} - \beta_{0,b}) = 0$ for all a, b.
(iv) The clusters of $f(x)$ are the whole set of roots R, sets $\{\beta_{i,1}, \ldots, \beta_{i,q_i}\}$ for every $i \neq 0$ and singleton roots.
(v) For $\mathfrak{s} = R$, the inertia subgroup I_F acts trivially on $\mathbb{C}[\mathfrak{s}_0]$ and $\gamma_{\mathfrak{s}} = \epsilon_{\mathfrak{s}} = \mathbf{1}$.
(vi) For $\mathfrak{s} = \{\beta_{i,1}, \ldots, \beta_{i,q_i}\}$ with $i \neq 0$, the inertia subgroup I_F acts tamely on $\mathbb{C}[\mathfrak{s}_0]$ and the eigenvalues of a generator τ of tame inertia are precisely the q_i-th roots of unity. Moreover, $\gamma_{\mathfrak{s}}$ and $\epsilon_{\mathfrak{s}}$ are also tame and

$$\gamma_{\mathfrak{s}}(\tau) = \begin{cases} 1 \text{ if } t \text{ is even} \\ -1 \text{ if } t \text{ is odd,} \end{cases} \qquad \epsilon_{\mathfrak{s}}(\tau) = \begin{cases} 0 \text{ if } q_i \neq 2 \\ \mathbf{1} \text{ if } q_i = 2. \end{cases}$$

Proof. (i) The roots of $g_i(x)$ all reduce to 0 in $\overline{\mathbb{F}}$, so those of $g_i(x - \alpha_i)$ all reduce to $\overline{\alpha_i}$. The result follows as $\overline{\alpha_i} \neq \overline{\alpha_j}$ for $i \neq j$ and $\overline{\alpha_i} \neq \overline{\beta}_{0,j}$ for all i, j.
(ii) This follows from Lemma 2.5.
(iii) The statement follows from the definition of type $t - \{q_1, \ldots, q_k\}$ and of $h(x)$.
(iv) Clear from (i), (ii) and (iii).
(v) I_F acts trivially on the roots of $h(x)$ and on $\{\alpha_1, \ldots, \alpha_k\}$, and hence trivially on $\mathbb{C}[\mathfrak{s}_0]$. Here $\mu_{\mathfrak{s}} = d_{\mathfrak{s}} = \lambda_{\mathfrak{s}} = 0$, so $\gamma_{\mathfrak{s}} = \epsilon_{\mathfrak{s}} = \mathbf{1}$.
(vi) The result for $\mathbb{C}[\mathfrak{s}_0] = \mathbb{C}[\mathfrak{s}]$ follows from Lemma 2.5. By (ii) $d_{\mathfrak{s}} = \frac{t}{q_i}$, $\mu_{\mathfrak{s}} = 0$ so $\lambda_{\mathfrak{s}} = \frac{1}{2}(\mu_{\mathfrak{s}} + d_{\mathfrak{s}}|\mathfrak{s}_0|) = \frac{t}{2}$. Therefore $\gamma_{\mathfrak{s}}$ is either trivial or it has order 2 depending on the parity of t. Since $\mu_{\mathfrak{s}} = 0$, $\epsilon_{\mathfrak{s}}$ is tame and

$$\epsilon_{\mathfrak{s}}(\tau) = \begin{cases} 0 \text{ if } q_i \neq 2 \\ \mathbf{1} \text{ if } q_i = 2. \end{cases}$$

□

Proof of Theorem 2.1. By Lemma 2.6 (iv) the set X of clusters of $f(x)$ which are not singletons nor unions of even clusters consists of the whole set of roots R and $\{\beta_{i,1}, \ldots, \beta_{i,q_i}\}$ for every $i \neq 0$, with $\beta_{i,j}$ as in Lemma 2.6.

The inertia group I_F does not permute the clusters so by Theorem 2.3 we have $H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell) \cong H^1_{ab} \oplus (H^1_t \otimes \mathrm{Sp}(2))$ with $H^1_{ab} = \bigoplus_{\mathfrak{s} \in X} V_{\mathfrak{s}}$ and $H^1_t = (\bigoplus_{\mathfrak{s} \in X} \epsilon_{\mathfrak{s}}) \ominus \epsilon_R = 0$, where the last equality follows from Lemma 2.6 (vi) since $q_i \neq 2$ for all i.

By Lemma 2.6 (v) and (vi), $V_{\mathfrak{s}}$ is tame for each cluster $\mathfrak{s}$.

For $\mathfrak{s} = R$, by Lemma 2.6 (v) inertia acts trivially on V_R.

For $\mathfrak{s} = \{\beta_{i,1}, \dots, \beta_{i,q_i}\}$, by Lemma 2.6 (vi) the eigenvalues of τ on $V_{\mathfrak{s}}$ are $\zeta_{q_i}, \zeta_{q_i}^2, \dots, \zeta_{q_i}^{q_i-1}$ or $-\zeta_{q_i}, -\zeta_{q_i}^2, \dots, -\zeta_{q_i}^{q_i-1}$ depending on whether t is even or odd respectively. In particular, τ acts semisimply on $H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell)$ by an element of order dividing $2\prod_i q_i$. This proves the claim about the action of inertia on $H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell)$.

As $\ell \neq p$, $H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell)$ is the dual of $T_\ell(J) \otimes \mathbb{Q}_\ell$ as an I_F-representation. In particular, the action of I_F on $T_\ell(J)$ factors through the same tame quotient and τ has the same set of eigenvalues. The result for $J[\ell]$ follows by reducing the characteristic polynomial of τ modulo ℓ. □

2.2. $J[\ell]$ when $\ell = p$: fundamental characters.

Given an abelian variety A/F with semistable reduction, a result due to Raynaud allows us to recover the eigenvalues of a generator of the tame inertia group acting on $A[p]$. Recall that for an integer d coprime to p, we write ζ_d for a primitive d-th root of unity, chosen such that for all divisors d' of d we have $\zeta_d^{d'} = \zeta_{\frac{d}{d'}}$.

Theorem 2.7. *Let A/F be an abelian variety with semistable reduction. Then the eigenvalues of a generator of the tame inertia group on $A[p]$ are all of the form*

$$\zeta_{p^n-1}^{\sum_{i=0}^{n-1} a_i p^i}$$

for $1 \leq n \leq 2\dim(A)$ and $0 \leq a_i \leq e_F$, and where the ζ_d form some compatible system of roots of unity.

For ease of reading, we will recall briefly the theory of fundamental characters. For further details see [Ser72, §1].

Let I_t denote the tame inertia quotient of I_F. A surjective homomorphism $\psi_n : I_t \to \mathbb{F}_{p^n}^\times$ defined by

$$\psi_n(\sigma) = \frac{\sigma(\pi_n)}{\pi_n} \bmod \pi_n \quad \text{where } \pi_n = (\pi_F)^{1/(p^n-1)},$$

is a fundamental character of level n. The set of fundamental characters of level n is the set of the n characters ψ_n, $\psi_n^p, \dots, \psi_n^{p^{n-1}}$; this set is independent of the choice of $(\pi_F)^{1/(p^n-1)}$. The fundamental characters of level n satisfy compatibility relations with fundamental characters of level m for any integer m dividing n:

$$\psi_n(\tau)^{\frac{p^n-1}{p^m-1}} = \psi_m(\tau), \quad \text{for all } \tau \in I_t.$$

Proof of Theorem 2.7. Let V be a Jordan-Hölder factor of dimension n over $\mathbb{F}_p$ of the I_F-module $A[p]$. Then, by [Ray74, Corollaire 3.4.4], V has the structure of a 1-dimensional $\mathbb{F}_{p^n}$-vector space with the action of I_F given by a character $\varpi : I_F \to \mathbb{F}_{p^n}^\times$, where

$$\varpi = \psi_n^{\sum_{i=0}^{n-1} a_i p^i}$$

with $0 \leq a_i \leq e_F$.

Let τ be a fixed generator of tame inertia. Then $\psi_n(\tau) = \zeta_{p^n-1} \in \mathbb{F}_{p^n}^\times$ and $\varpi(\tau)$ acts as multiplication by $\zeta_{p^n-1}^{\sum_{i=0}^{n-1} a_i p^i}$ on $\mathbb{F}_{p^n}$.

Let Φ be the minimal polynomial of ζ_{p^n-1} over $\mathbb{F}_p$. Since $\mathbb{F}_p[\zeta_{p^n-1}] \cong \mathbb{F}_{p^n}$, the minimal polynomial Φ has degree n and hence its roots are

$$\zeta_{p^n-1}, \zeta_{p^n-1}^p, \zeta_{p^n-1}^{p^2}, \dots, \zeta_{p^n-1}^{p^{n-1}}.$$

Therefore, by the Cayley-Hamilton theorem, these are precisely the eigenvalues of multiplication by ζ_{p^n-1} on V.

Hence, the eigenvalues of $\varpi(\tau)$ are $\zeta_{p^n-1}^{\sum_{i=0}^{n-1} a_i p^i}$. □

2.3. **Creating a transvection.**

Finally, we will need a criterion to ensure that some element of $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q})$ acts as a transvection on $J[\ell]$. We again use inertia groups for achieving this.

Definition 2.8. Recall that a *transvection* in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is a unipotent element σ such $\sigma - \mathrm{Id}_{2g\times 2g}$ has rank 1.

Lemma 2.9. *Suppose that $p \nmid 2\ell$ and $f(x) \in \mathcal{O}_F[x]$ has type $1-\{2\}$. Then some element of I_F acts as a transvection on $J[\ell]$.*

Proof. The model of the curve consisting of the chart $y^2 = f(x)$ and the usual chart at infinity is a regular proper semistable model of C. The dual graph of the special fibre is a vertex with a loop. The homology group of the dual graph is $\mathbb{Z}$ with intersection pairing (1), so the Tamagawa number of the Jacobian over K^{nr} is $c(J/K^{nr}) = \det(1) = 1$ (see e.g. [Pap13, Theorem 3.5 and Theorem 3.8]).

On the other hand, for a principally polarised g-dimensional semistable abelian variety A of toric dimension d, the inertia group acts on $T_\ell(A)$ by block matrices of the form

$$\sigma \mapsto \begin{pmatrix} \mathrm{Id}_d & 0 & t_\ell(\sigma)N \\ 0 & \mathrm{Id}_{2g-2d} & 0 \\ 0 & 0 & \mathrm{Id}_d \end{pmatrix}$$

where t_ℓ is the ℓ-adic tame character and N is a $d \times d$ symmetric integer-valued matrix that satisfies $c(A/K^{nr}) = |\mathrm{coker}(N)|$ (it is the matrix induced by the monodromy pairing composed with the principal polarisation on A); see e.g. [GR72, § 9,§ 10] or the summary in [DD09, § 3.5.1]. In our case $d = 1$ and $c(J/K^{nr}) = 1$, so N is a 1×1 matrix with entry 1. In particular, picking σ appropriately gives an element of the inertia group that acts on $J[\ell]$ as a transvection. □

3. Irreducibility

The aim of this section is to provide explicit criteria on $f(x)$ that force irreducibility of the mod ℓ Galois representation. The key idea is to ensure that images of local Galois groups are sufficiently large and can be patched together to guarantee global irreducibility.

3.1. **Local representations.**

Proposition 3.1. *Let $C : y^2 = f(x)$ be a hyperelliptic curve over a local field F of odd residue characteristic p, with $f(x) \in \mathcal{O}_F[x]$ monic and squarefree, and let $J = \mathrm{Jac}(C)$. Suppose that $f(x)$ has type $t - \{q_1, \ldots, q_k\}$ where $q_1, \ldots, q_k$ are odd primes, coprime to t. Suppose moreover that the size of the residue field $\#\mathbb{F}$ is a primitive root modulo each of the q_i. Then for every prime $\ell \neq p, q_1, \ldots, q_k$, the semisimple representation $(J[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell)_{ss}$ decomposes as a direct sum of one (q_1-1)-dimensional, one (q_2-1)-dimensional, …, one (q_k-1)-dimensional irreducible G_F-subrepresentation, and all other irreducible constituents being 1-dimensional.*

Proof. By Theorem 2.1, G_F acts tamely on $J[\ell]$ and the non-trivial eigenvalues of a generator of tame inertia are $\pm\zeta_{q_i}^{r_{i,j}}$ for $r_{i,j}=1,\dots,q_i-1$, where each sign is $+$ if t is even and $-$ if t is odd. We claim that the conclusion of the proposition holds for any semisimple $\overline{\mathbb{F}}_\ell$-representation V with this property.

The action on V factors through a finite group $G=\langle\tau,\phi\rangle$, where $\langle\tau\rangle\lhd G$ is the (tame) inertia subgroup and ϕ is any lift of Frobenius.

Write V_z for the z-eigenspace of τ on V. Since $\phi\tau\phi^{-1}=\tau^{\#\mathbb{F}}$, and hence $\tau\phi^{-1}=\phi^{-1}\tau^{\#\mathbb{F}}$, it follows that ϕ^{-1} maps V_z to $V_{z^{\#\mathbb{F}}}$. In particular, $\phi^{-(q_i-1)}$ is an endomorphism of $V_{\pm\zeta_{q_i}}$.

Pick $v\in V_{\pm\zeta_{q_i}}$ which is an eigenvector for the action of $\phi^{-(q_i-1)}$ on $V_{\pm\zeta_{q_i}}$ and consider the subspace $W=\langle v,\phi^{-1}v,\dots,\phi^{-(q_i-2)}v\rangle$. Since W is closed under τ and ϕ^{-1}, it is a G_F-submodule of V.

Moreover, as $\#\mathbb{F}$ is a primitive root modulo q_i, it follows that the eigenvalues of τ on $\langle v\rangle,\dots,\langle\phi^{-(q_i-2)}v\rangle$ are precisely the non-trivial q_i-th roots of unity, or their negatives. In particular, as these τ-eigenvalues are distinct, any G-submodule of W must be a direct sum of some of the $\langle\phi^j v\rangle$'s. As ϕ^{-1} permutes these τ-eigenspaces transitively, it therefore follows that W is irreducible.

Now the result follows by substituting V by V/W and then proceeding by induction on the dimension. □

3.2. **Global representations.**

Lemma 3.2. *Let $C: y^2=f(x)$ be a hyperelliptic curve over a number field K, where $f(x)\in\mathcal{O}_K[x]$ is a monic squarefree polynomial of degree $2g+2$. Suppose that $f(x)$ has type $t-\{q_1,q_2\}$ at $\mathfrak{p}_2$ and type $t'-\{q_3\}$ at $\mathfrak{p}_3$, where:*

- *q_1, q_2 and q_3 are primes with $q_1\le q_2<q_3<2g+2$ and $q_1+q_2=2g+2$;*
- *$\mathfrak{p}_2,\mathfrak{p}_3\nmid 2$;*
- *t is coprime to q_1q_2, and t' is coprime to q_3;*
- *$\#\mathbb{F}_{\mathfrak{p}_2}$ is a primitive root modulo q_1 and q_2;*
- *$\#\mathbb{F}_{\mathfrak{p}_3}$ is a primitive root modulo q_3.*

Then for every prime $\ell\nmid q_1,q_2,q_3,\#\mathbb{F}_{\mathfrak{p}_2},\#\mathbb{F}_{\mathfrak{p}_3}$, the G_K-module $J[\ell]$ is absolutely irreducible, where J is the Jacobian of C.

Proof. By Proposition 3.1, the restriction of $J[\ell]\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ to $G_{K_{\mathfrak{p}_3}}$ contains an irreducible (q_3-1)-dimensional subquotient. Also its restriction to $G_{K_{\mathfrak{p}_2}}$ has exactly two Jordan-Holder factors and these have dimension (q_1-1) and (q_2-1). It follows that, on the one hand, $J[\ell]\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ can have at most two Jordan-Holder factors, in which case they have dimensions (q_1-1) and (q_2-1), and, on the other hand, $J[\ell]\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ has a Jordan-Holder factor of dimension at least (q_3-1). Hence $J[\ell]\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ is irreducible. □

Theorem 3.3. *Let $C: y^2=f(x)$ be a hyperelliptic curve over a number field K, where $f(x)\in\mathcal{O}_K[x]$ is a monic squarefree polynomial of degree $2g+2$. Suppose that $f(x)$ has type $t-\{q_1,q_2\}$ at $\mathfrak{p}_2$, type $t'-\{q_4,q_5\}$ at $\mathfrak{p}_2'$, type $t''-\{q_3\}$ at $\mathfrak{p}_3$, and type $t'''-\{q_5\}$ at $\mathfrak{p}_3'$, where:*

- *q_1,q_2,q_3,q_4 and q_5 are primes such that:*

$$2g+2=q_1+q_2=q_4+q_5\qquad q_4<q_1\le q_2<q_5<q_3<2g+2;$$

- *$\mathfrak{p}_2,\mathfrak{p}_2',\mathfrak{p}_3,\mathfrak{p}_3'\nmid 2\prod_i q_i$ and they have distinct residue characteristics;*

- *t is coprime to q_1q_2; t' is coprime to q_4q_5; t'' is coprime to q_3 and t''' is coprime to q_5;*
- *$\#\mathbb{F}_{\mathfrak{p}_2}$ is a primitive root modulo q_1 and q_2;*
- *$\#\mathbb{F}_{\mathfrak{p}_2'}$ is a primitive root modulo q_4 and q_5;*
- *$\#\mathbb{F}_{\mathfrak{p}_3}$ is a primitive root modulo q_3;*
- *$\#\mathbb{F}_{\mathfrak{p}_3'}$ is a primitive root modulo q_5.*

Then for every prime ℓ, the G_K-module $J[\ell]$ is absolutely irreducible, where J is the Jacobian of C.

Proof. Applying Lemma 3.2 with $q_1, q_2, q_3, \mathfrak{p}_2, \mathfrak{p}_3$ proves the claim for all ℓ with $\mathfrak{p}_2, \mathfrak{p}_3, q_1, q_2, q_3 \nmid \ell$. Applying the lemma again with $q_4, q_5, q_3, \mathfrak{p}_2', \mathfrak{p}_3$ proves it for all ℓ with $\mathfrak{p}_3, q_3 \nmid \ell$. By assumption $q_5 > q_1, q_2$, so applying the lemma with $q_1, q_2, q_5, \mathfrak{p}_2, \mathfrak{p}_3'$ proves the result for $\mathfrak{p}_3, q_3 \mid \ell$. □

4. Primitivity

In this section K is a number field and $C\colon y^2 = f(x)$ a hyperelliptic curve over K, where $f(x) \in \mathcal{O}_K[x]$ is a monic squarefree polynomial of degree $2g+2$. As before, $J = \mathrm{Jac}(C)$. In this section moreover $\mathfrak{p}$ will denote a prime of K.

Definition 4.1. Let V be a symplectic vector space over a field, and let G be a subgroup of $\mathrm{GSp}(V)$. We say that $\{V_1, \ldots, V_k\}$ is a *non-trivial G-stable decomposition of V into symplectic subspaces* if the V_i are proper symplectic subspaces $V_i \subset V$, the symplectic pairing is non-degenerate on V_i, and there is a homomorphism $\phi : G \to S_k$ such that $V = \oplus_{i=1}^k V_i$ and $\sigma(V_i) = V_{\phi(\sigma)(i)}$ for $\sigma \in G$.

Definition 4.2. Let V be a symplectic vector space over a field, and let G be a subgroup of $\mathrm{GSp}(V)$. Suppose that V has no proper G-stable subspace. Recall that V is an *imprimitive* G-module if there is no non-trivial G-stable decomposition of V into symplectic subspaces. If V is not an imprimitive G-module, then it is a *primitive* G-module.

4.1. Quasi-unramified representations.

Definition 4.3 (Quasi-unramified representation)**.** We will say that a symplectic $\mathbb{F}_\ell$-representation V of G_K is *quasi-unramified* if for every G_K-stable decomposition $V = \oplus_{i=1}^k V_i$ into symplectic $\mathbb{F}_\ell$-subspaces, the permutation action of G_K on $\{V_1, \ldots, V_k\}$ is unramified at every prime of K. We will say that V is *strongly quasi-unramified* if the same condition holds for decompositions of $V \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell$ into symplectic $\overline{\mathbb{F}}_\ell$-subspaces.

Note that strongly quasi-unramified implies quasi-unramified.

Proposition 4.4. *Let K be a number field which does not have everywhere unramified extensions. If V is an irreducible quasi-unramified symplectic representation of G_K, then V is primitive.*

Proof. Suppose V admits a G_K-stable decomposition into symplectic subspaces. Since V is irreducible, the associated homomorphism ϕ is transitive and, in particular, non-trivial. By definition of quasi-unramified symplectic representation, the kernel of ϕ cuts out a proper unramified extension of K. Hence, V is primitive. □

Remark 4.5. By the Hermite-Minkowski theorem, $\mathbb{Q}$ satisfies the hypotheses of Proposition 4.4. Similarly, the same holds for $\mathbb{Q}(\zeta_3)$.

4.2. **Criteria for being quasi-unramified.**

Definition 4.6 (Admissible polynomials)**.** We will say that $f(x) \in \mathcal{O}_K[x]$ is *ℓ-admissible at $\mathfrak{p}$* if for every G_K-stable decomposition $J[\ell] \otimes \overline{\mathbb{F}}_\ell = \oplus_{i=1}^k V_i$ into symplectic $\overline{\mathbb{F}}_\ell$-subspaces, $I_\mathfrak{p}$ acts trivially on $\{V_1, \dots, V_k\}$.

We will say that $f(x) \in \mathcal{O}_K[x]$ is *admissible at $\mathfrak{p}$* if it is ℓ-admissible at $\mathfrak{p}$ for every odd prime number ℓ not divisible by $\mathfrak{p}$.

Proposition 4.7. *Let ℓ be an odd prime number and suppose that:*
(1) $f(x)$ is admissible at all $\mathfrak{p} \nmid \ell$;
(2) $f(x)$ is ℓ-admissible at all $\mathfrak{p} \mid \ell$.
Then $J[\ell]$ is strongly quasi-unramified.

Proof. Direct from the definition. □

The following criterion is another way of ensuring that $J[\ell]$ is quasi-unramified for certain primes ℓ:

Proposition 4.8. *If $J[\ell]$ is irreducible and there exists a prime number q such that*

- *$g+1 < q < 2g+2$;*
- *ℓ is a primitive root modulo q;*
- *f has type $t - \{q\}$ at $\mathfrak{p}$ for some $\mathfrak{p} \nmid 2\ell q t$;*

then $J[\ell]$ is quasi-unramified.

Proof. Suppose that $J[\ell] = \oplus_{i=1}^k V_i$ is a non-trivial G_K-stable decomposition into symplectic $\mathbb{F}_\ell$-subspaces. Since $J[\ell]$ is irreducible and the V_i are symplectic subspaces, $\dim V_i = \dim V_j \geq 2$. In particular, $k < g+1 < q$. By Theorem 2.1, $I_\mathfrak{p}$ acts on $J[\ell]$ through a cyclic quotient $\langle \tau \rangle \cong C_q$ or C_{2q}, with τ^2 having eigenvalues all the primitive q-th roots of unity, and all other eigenvalues 1. By hypothesis $k < q$, so τ^2 has to preserve each of the V_i. Without loss of generality $\tau^2 : V_1 \to V_1$ has ζ_q as an eigenvalue. The minimal polynomial of ζ_q over $\mathbb{F}_\ell$ has degree $q-1$, so $\frac{2g}{k} = \dim V_1 \geq q-1 > g$, and so $k = 1$. □

In the rest of this section we will give criteria for $f(x)$ to satisfy the hypotheses of Proposition 4.7.

4.3. **Admissible polynomials.**

Lemma 4.9. *If J is semistable at $\mathfrak{p}$ then $f(x)$ is admissible at $\mathfrak{p}$.*

Proof. Let ℓ be an odd prime with $\mathfrak{p} \nmid \ell$. Suppose that $J[\ell] \otimes \overline{\mathbb{F}}_\ell = \oplus_{i=1}^k V_i$ is a non-trivial G_K-stable decomposition of $J[\ell] \otimes \overline{\mathbb{F}}_\ell$ into symplectic $\overline{\mathbb{F}}_\ell$-subspaces.

By [GR72, Corollaire 3.5.2], $I_\mathfrak{p}$ acts unipotently on $J[\ell]$ with $(\sigma - 1)^2 = 0$ for all $\sigma \in I_\mathfrak{p}$. By Lemma 4.16, every $\sigma \in I_\mathfrak{p}$ fixes each of the V_i and so $f(x)$ is ℓ-admissible at $\mathfrak{p}$. □

Lemma 4.10. *Let $\mathfrak{p}$ be a prime of odd residue characteristic p. If $f(x) \in \mathcal{O}_K[x]$ has type $t - \{q_1, q_2\}$ at $\mathfrak{p}$ for t odd and odd primes q_1, q_2 different from p, with $q_1 + q_2 = 2g+2$, then $f(x)$ is admissible at $\mathfrak{p}$.*

Proof. Let $\ell \neq 2, p$ be a prime. Suppose that $J[\ell] \otimes \overline{\mathbb{F}}_\ell = \oplus_{i=1}^k V_i$ is a non-trivial G_K-stable decomposition into symplectic $\overline{\mathbb{F}}_\ell$-subspaces. By Theorem 2.1, $I_\mathfrak{p}$ acts tamely on $J[\ell]$ through a cyclic quotient of order dividing $2q_1q_2$. Let τ be a fixed

generator of tame inertia. We need to show that τ acts trivially on $\{V_1, \dots, V_k\}$. Again by Theorem 2.1, τ has eigenvalues $-\zeta_{q_1}, \dots, -\zeta_{q_1}^{q_1-1}, -\zeta_{q_2}, \dots, -\zeta_{q_2}^{q_2-1}$.

If $\ell \neq q_1, q_2$, then no subset of the eigenvalues is closed under multiplication by either -1, ζ_{q_1} or ζ_{q_2}, and so by Lemma 4.15, τ cannot permute $\{V_1, \dots, V_k\}$.

If $\ell = q_1 \neq q_2$, then by the same argument τ cannot have an orbit on $\{V_1, \dots, V_k\}$ of length 2. Moreover, τ does not have an eigenvalue of multiplicity q_1, so by Lemma 4.15 τ cannot have an orbit of lenght divisible by q_1. Furthermore, no set of $2q_2$ eigenvalues is closed under multiplication by ζ_{q_2} and the V_i are symplectic (even dimension), so τ cannot have an orbit of length divisible by q_2 either.

Finally, if $\ell = q_1 = q_2 = g + 1$, then τ cannot cyclically permute q_1 symplectic subspaces since $\dim_{\mathbb{F}_\ell} J[\ell] = 2g < 2q_1$. It also cannot have an orbit of length 2 as no subset of the eigenvalues is closed under multiplication by -1. □

Lemma 4.11. *Let $\mathfrak{p}$ be a prime of odd residue characteristic p. If $f(x) \in \mathcal{O}_K[x]$ has type $2-\{q\}$ at $\mathfrak{p}$ where q is an odd prime $g+1 < q < 2g+2$, then $f(x)$ is admissible at $\mathfrak{p}$.*

Proof. Let $\ell \neq 2, p$ be a prime. By Theorem 2.1, $I_\mathfrak{p}$ acts tamely on $J[\ell]$ through a cyclic quotient of order dividing $2q$, and with a generator of tame inertia τ having non-trivial eigenvalues $\zeta_q, \dots, \zeta_q^{q-1}$, each with multiplicity 1 (unless $\ell = q$ in which case all eigenvalues are $+1$).

Since $\ell \neq 2$, the order of the image of $I_\mathfrak{p}$ is q or 1. Clearly, since $q > g+1$, inertia cannot permute q symplectic blocks. □

4.4. p-admissible polynomials.

Let us address condition (2) in Proposition 4.7.

Proposition 4.12. *If C/K is semistable at $\mathfrak{p}$ of residue characteristic p, with*

$$p > \max(g, 2e_{K_\mathfrak{p}} + 1),$$

where $e_{K_\mathfrak{p}}$ is the ramification degree of $K_\mathfrak{p}/\mathbb{Q}_p$, then $f(x)$ is p-admissible at $\mathfrak{p}$.

Proof. Suppose that $J[p] \otimes \overline{\mathbb{F}}_p = \oplus_{i=1}^m V_i$ is a non-trivial $G_{K_\mathfrak{p}}$-stable decomposition into symplectic subspaces.

As $p > g$ the wild inertia group cannot permute the subspaces, as each orbit must have either size 1 or size divisible by p.

By Theorem 2.7, the eigenvalues of a (fixed) generator τ of the tame inertia group are of the form $\zeta_{p^k-1}^{\sum_{i=0}^{k-1} a_i p^i}$ for some $1 \leq k \leq 2 \dim J$ and $0 \leq a_i \leq e_{K_\mathfrak{p}}$. In particular, if ζ_x is a root of unity such that $\zeta_x^{\frac{x}{p^k-1}} = \zeta_{p^k-1}$ for all k, then each eigenvalue is of the form

$$\zeta_x^{tx} \qquad \text{for some} \quad 0 \leq t \leq \frac{e_{K_\mathfrak{p}}}{p-1} < \frac{1}{2}.$$

This set has no subset closed under multiplication by j-th roots of unity for any $j \leq g$ (as $g < p$). Thus by Lemma 4.15, τ cannot permute $\{V_1, \dots, V_m\}$. □

Remark 4.13. The result and the proof of Proposition 4.12 also hold for abelian varieties. Let A be a g-dimensional semistable abelian variety over a local field $F/\mathbb{Q}_p$. Suppose that $A[p] \otimes \overline{\mathbb{F}}_p = \oplus_{i=1}^m V_i$ is a G_F-stable decomposition into symplectic subspaces. If $p > \max(g, 2e_F + 1)$ then I_F does not permute $\{V_1, \dots, V_m\}$.

Proposition 4.14. *Let $\mathfrak{p}$ be a prime of odd residue characteristic p with*

$$e_{K_\mathfrak{p}(\zeta_p)/K_\mathfrak{p}} \neq 2.$$

If J has totally toric reduction at $\mathfrak{p}$ then $f(x)$ is p-admissible at $\mathfrak{p}$.

Proof. Suppose that $J[p] \otimes \overline{\mathbb{F}}_p = \oplus_{i=1}^k V_i$ is a G_K-stable decomposition of $J[p]$ into symplectic $\overline{\mathbb{F}}_p$-subspaces. The inertia group $I_\mathfrak{p}$ acts on $T_p(J)$ as

$$\sigma \mapsto \left(\begin{array}{c|c} \chi(\sigma)\operatorname{Id}_{g\times g} & * \\ \hline 0 & \operatorname{Id}_{g\times g}\end{array}\right),$$

where χ is the cyclotomic character (as follows from the Raynaud parametrization $J(\overline{K}_\mathfrak{p}) \cong (\overline{K}_\mathfrak{p}^\times)^g/\text{lattice}$, so that $0 \to (\mu_{p^n})^g \to J(\overline{K}_\mathfrak{p})[p^n] \to (\mathbb{Z}/p^n)^g \to 0$). In particular, the action of $I_\mathfrak{p}$ on $J[p]$ factors through a group of the form $G = W \rtimes H$, where W consists of unipotent matrices, and $H = \langle\tau\rangle$ is a cyclic group of order $e_{K_\mathfrak{p}(\zeta_p)/K_\mathfrak{p}}$. The eigenvalues of τ are 1 and $\chi(\tau)$, both with multiplicity g.

Since W is a p-group with all elements satisfying $(M-\operatorname{Id})^2 = 0$, by Lemma 4.16, W acts trivially on $\{V_1, \dots, V_k\}$. Since $\chi(\tau) \neq -1$, the eigenvalues of τ have no subset closed under multiplication by any root of unity. Thus, by Lemma 4.15 τ cannot permute any of the V_i either. Therefore, $I_\mathfrak{p}$ acts trivially on $\{V_1, \dots, V_k\}$, as required.

□

4.5. **Miscellaneous linear algebra.**

Lemma 4.15. *Let $V = \oplus_{i=1}^k V_i$ be a finite dimensional vector space over a field L. Let $T\colon V \to V$ be an L-linear map such that $T(V_i) = V_{i+1}$ (the indices considered modulo k). If the eigenvalues of T^k on V_1 are $\alpha_1, \dots, \alpha_d$ (with multiplicity), then the eigenvalues of T on V (with multiplicity) are*

$$\zeta_k^j \sqrt[k]{\alpha_i}$$

for $i = 1, \dots, d$ and $j = 0, \dots, k-1$.

Proof. Without loss of generality, suppose that L is algebraically closed. Pick $v \in V$ such that $Tv = \beta v$. Write $v = \sum_{i=1}^k v_i$ for $v_i \in V_i$, so $Tv_i = \beta v_{i+1}$.

On the subspace $W = \langle v_1, \dots, v_k\rangle$ the map T^k acts as multiplication by β^k, so $T^k - \beta^k = 0$ on W. The minimal polynomial of T on W must have at least degree k, so by the Cayley-Hamilton theorem the characteristic polynomial of T on W is $x^k - \beta^k$. Hence its eigenvalues are $\zeta_k^j\beta$ for $j = 0, \dots, k-1$. Now take $V' = V/W = \oplus_{i=1}^k V_i/\langle v_i\rangle$ and proceed by induction on the dimension. □

Lemma 4.16. *Let ℓ be an odd prime and V an $\overline{\mathbb{F}}_\ell$-vector space. Suppose $M : V \to V$ is a linear map and satisfies $(M - \operatorname{Id})^2 = 0$. Then there is no set of linearly independent subspaces $V_1, \dots, V_k$ of V (for $k > 1$) which are cyclically permuted by M.*

Proof. Since $0 = (M - \operatorname{Id})^\ell = M^\ell - \operatorname{Id}$, either $M = \operatorname{Id}$ or M has order ℓ. So, if it permutes a set of linearly independent subspaces $V_1, \dots, V_k$ cyclically, then $k = \ell > 2$. Now if $v \in V_1 \setminus \{0\}$, then

$$0 = (M - \operatorname{Id})^2 v = M^2 v - 2Mv + v,$$

which gives a contradiction since $v \in V_1 \setminus \{0\}$, $2Mv \in V_2$ and $M^2 v \in V_3$. □

5. Surjectivity

5.1. Generating symplectic groups.

We make use of the following classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ containing a transvection, due to Hall and Arias-de-Reyna, Dieulefait, Wiese.

Theorem 5.1 ([Hal08, Theorem 1.1]; [ADW16, Theorem 1.1])**.** *Let $\ell \geq 5$ be a prime and let V be a symplectic $\mathbb{F}_\ell$-vector space. Let G be a subgroup of $\mathrm{GSp}(V)$ such that:*

(i) G contains a transvection;
(ii) V is an $\mathbb{F}_\ell$-irreducible G-module;
(iii) V is a primitive G-module.

Then G contains the symplectic group $\mathrm{Sp}(V)$. The same is true for $\ell = 3$, provided that $V \otimes \overline{\mathbb{F}}_3$ is an irreducible and primitive G-module.

Proposition 5.2. *If $\ell \geq 5$ and V is an irreducible quasi-unramified symplectic representation of $G_\mathbb{Q}$, then the image of $G_\mathbb{Q}$ contains $\mathrm{Sp}(V)$ provided that some element of $G_\mathbb{Q}$ acts as a transvection. The same holds for $\ell = 3$ provided that V is also absolutely irreducible and strongly quasi-unramified.*

Proof. By Lemma 4.4 the representation is primitive. The result follows from Theorem 5.1. □

5.2. Symplectic representations and abelian varieties.

Theorem 5.3. *Let $\ell \geq 5$ be a prime and let A/K be a principally polarized abelian variety of dimension g over a number field K. If the G_K-action on $A[\ell]$ is irreducible, primitive and contains a transvection, then the image of G_K contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. Moreover, the same holds for $\ell = 3$ provided that $A[3] \otimes \overline{\mathbb{F}}_3$ is also irreducible.*

Proof. The result follows directly from Theorem 5.1. □

Lemma 5.4. *Let ℓ be a prime and let A/K be a principally polarized abelian variety of dimension g over a number field K. Let $G = \mathrm{Gal}(K(A[\ell])/K)$. Then $[G : G \cap \mathrm{Sp}_{2g}(\mathbb{F}_\ell)] = [\mathbb{Q}(\zeta_\ell) : K \cap \mathbb{Q}(\zeta_\ell)]$.*

Proof. Let $t : \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times$ be the group homomorphism which maps an element $M \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ to the corresponding multiplier through the symplectic pairing, that is the element $m \in \mathbb{F}_\ell^\times$ such that for all $u, v \in \mathbb{F}_\ell^{2g}$, $\langle Mu, Mv\rangle = m\langle u, v\rangle$. The kernel of this homomorphism is $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Since the abelian variety is principally polarized, the symplectic pairing on $J[\ell]$ is the mod ℓ Weil pairing: for all $\sigma \in G_K$ and for all $v, w \in J[\ell]$ we have $\langle \sigma v, \sigma w\rangle = \chi(\sigma)\langle v, w\rangle$. Therefore the homomorphism t restricted to G is the cyclotomic character and

$$[G : G \cap \mathrm{Sp}_{2g}(\mathbb{F}_\ell)] = |\text{image of } \chi \text{ on } G| = [\mathbb{Q}(\zeta_\ell) : K \cap \mathbb{Q}(\zeta_\ell)].$$

□

Corollary 5.5. *Let $\ell \geq 5$ be a prime and let J/K be the Jacobian of a curve of genus g over a number field K. If the G_K-action on $J[\ell]$ is irreducible, primitive and contains a transvection, then $\mathrm{Gal}(K(J[\ell])/K)$ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ with index*

$[\mathbb{Q}(\zeta_\ell) : K \cap \mathbb{Q}(\zeta_\ell)]$. *Moreover, the same holds for* $\ell = 3$ *provided that* $J[3] \otimes \overline{\mathbb{F}}_3$ *is also irreducible.*

Proof. Since J is principally polarized (see [Mil86, Summary 6.11]), Theorem 5.3 implies that the image of G_K contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. The result follows from Lemma 5.4. □

Theorem 5.6. *Let* $\ell \geq 5$ *be a prime and let* $J/\mathbb{Q}$ *be the Jacobian of a curve of genus* g. *If the* $G_\mathbb{Q}$*-action on* $J[\ell]$ *is irreducible, quasi-unramified and contains a transvection, then* $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. *Moreover, the same holds for* $\ell = 3$ *provided that* $J[3]$ *is also absolutely irreducible and strongly quasi-unramified.*

Proof. By Lemma 4.4 the representation is primitive. The result follows from Corollary 5.5. □

6. Maximal Galois images over $\mathbb{Q}$

We now put together the results from § 2-§ 5 to produce hyperelliptic curves over $\mathbb{Q}$ with maximal Galois images. In this section $C\colon y^2 = f(x)$ denotes a hyperelliptic curve over $\mathbb{Q}$, where $f(x) \in \mathbb{Z}[x]$ is a monic squarefree polynomial of degree $2g+2$. As before, $J = \mathrm{Jac}(C)$.

For the rest of the section we will refer to the following hypotheses on the genus and on $f(x)$:

(G+ϵ) There exist primes q_1, q_2 and q_3 such that:

$$2g+2 = q_1 + q_2, \qquad q_1 \leq q_2 < q_3 < 2g+2.$$

(2G+ϵ) There exist primes q_1, q_2, q_3, q_4, q_5 such that:

$$2g+2 = q_1 + q_2 = q_4 + q_5, \qquad q_4 < q_1 \leq q_2 < q_5 < q_3 < 2g+2.$$

(2T) $f(x)$ has type $1-\{2\}$ at distinct primes $p_t, p_t' > g$.

(TT) J has totally toric reduction at all odd primes $\ell \leq g$.

(p_2) $f(x)$ has type $1-\{q_1, q_2\}$ at a prime $p_2 > 2g+2$, which is a primitive root modulo q_1, q_2 and q_3.

(p_3) $f(x)$ has type $2-\{q_3\}$ at a prime $p_3 > 2g+2$, which is a primitive root modulo q_3.

(p_2') $f(x)$ has type $1-\{q_4, q_5\}$ at a prime $p_2' > 2g+2$, which is a primitive root modulo q_3, q_4 and q_5.

(p_3') $f(x)$ has type $2-\{q_5\}$ at a prime $p_3' > 2g+2$, which is a primitive root modulo q_5.

(adm) $f(x)$ is admissible at all primes p (see Definition 4.6).

(ss) C is semistable at all primes $p \notin \{p_2, p_2', p_3, p_3'\}$.

(3) $p_2, p_3 \equiv 1 \bmod 3$.

(S_{2g+2}) There exist two primes p_{irr} and p_{lin} such that $f(x)$ modulo p_{irr} is irreducible, and $f(x)$ modulo p_{lin} factors as an irreducible polynomial times a linear factor.

Theorem 6.2 requires the Goldbach conjecture like hypothesis (G + ϵ) and produces curves with maximal mod ℓ Galois images at all but a small set of primes. Theorem 6.5 requires the stronger hypothesis (2G + ϵ) but guarantees maximality at all ℓ simultaneously.

Remark 6.1. Note that hypothesis (adm) is automatically satisfied if hypotheses (p_2), (p_3), (p_2'),(p_3') and (ss) hold. The polynomial $f(x)$ is admissible at all primes: Lemma 4.10 and 4.11 ensure admissibility at p_2, p_3, p_2' and p_3', while hypothesis (ss) and Lemma 4.9 guarantee admissibility at all other primes.

Theorem 6.2. *Suppose $f(x) \in \mathbb{Z}[x]$ satisfies* $(\mathrm{G}+\epsilon)$, (2T), (p_2), (p_3) *and* (adm). *Then* $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ *provided that $\ell \neq 2, 3, q_1, q_2, q_3, p_2, p_3$ and either*

(i) $\ell > g$ and $J/\mathbb{Q}_\ell$ is semistable, or
(ii) $J/\mathbb{Q}_\ell$ has totally toric reduction, or
(iii) ℓ is a primitive root modulo q_3.

Proof. By Lemma 2.9, Hypothesis (2T) ensures the existence of a transvection in $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q})$.

By $(\mathrm{G}+\epsilon)$, (p_2) and (p_3), the hypotheses of Lemma 3.2 are satisfied, so $J[\ell]$ is absolutely irreducible for every prime $\ell \neq q_1, q_2, q_3, p_2, p_3$.

In case (i), by Proposition 4.12 and hypothesis (adm), the conditions of Proposition 4.7 are satisfied, so $J[\ell]$ is strongly quasi-unramified.

In case (ii), by Proposition 4.14 and hypothesis (adm), the conditions of Proposition 4.7 are again satisfied, so $J[\ell]$ is strongly quasi-unramified.

In case (iii), since $J[\ell]$ is irreducible and hypothesis (p_3) holds, Proposition 4.8 shows that $J[\ell]$ is quasi-unramified.

Therefore, $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ by Theorem 5.6. □

Remark 6.3. The theorem can be easily extended to include $\ell = p_2$ and p_3 by requiring that there is a second pair of primes r_2, r_3 satisfying the same properties as p_2 and p_3 in hypotheses (p_2) and (p_3).

From Theorem 6.2 we have the following immediate corollary:

Corollary 6.4. *If $f(x)$ also satisfies* (TT) *then* $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ *for every prime ℓ, except possibly for*

(i) $\ell = 2, 3, q_1, q_2, q_3, p_2, p_3$, and
(ii) ℓ where $J/\mathbb{Q}_\ell$ is not semistable that are not primitive generators modulo q_3.

Theorem 6.5. *Suppose $f(x) \in \mathbb{Z}[x]$ satisfies* $(2\mathrm{G}+\epsilon)$, (2T), (p_2), (p_3), (p_2'),(p_3'), (TT) *and* (ss). *Then* $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ *for all primes $\ell \neq 2, 3$.*

Moreover, if $f(x)$ also satisfies (3) *then* $\mathrm{Gal}(\mathbb{Q}(J[3])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_3)$, *and if $f(x)$ satisfies* (S_{2g+2}) *then* $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q}) \cong S_{2g+2}$.

Proof. Case $\ell \geq 5$. The hypotheses of Theorem 3.3 are satisfied by $(2\mathrm{G}+\epsilon)$, (p_2), (p_3), (p_2') and (p_3'), so $J[\ell]$ is absolutely irreducible for every prime ℓ.

By hypothesis (2T), Lemma 2.9 ensures that for every prime ℓ there exists a transvection in $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q})$.

The polynomial $f(x)$ is admissible at all primes: Lemmas 4.10 and 4.11 ensure admissibility for p_2, p_3, p_2' and p_3', while hypothesis (ss) and Lemma 4.9 guarantee admissibility at all other primes.

If $\ell \leq g$, then J has totally toric reduction by hypothesis (TT). Since $\ell \geq 5$, we have that $e_{\mathbb{Q}_\ell(\zeta_\ell)/\mathbb{Q}_\ell} \neq 2$. Therefore, by Proposition 4.14 $J[\ell]$ is ℓ-admissible at ℓ. If $\ell > g$ and $\ell \notin \{p_2, p_3, p_2', p_3'\}$, then J is semistable at ℓ by hypothesis (ss) and so by Proposition 4.12 $J[\ell]$ is ℓ-admissible at ℓ.

If $\ell \notin \{p_2, p_3, p_2', p_3'\}$, then by Proposition 4.7 $J[\ell]$ is strongly quasi-unramified. If $\ell \in \{p_2, p_3, p_2', p_3'\}$, then Proposition 4.8 with $q = q_3$ (or q_5) and $p = p_3$ (or p_3') shows that $J[\ell]$ is quasi-unramified.

Therefore, by Theorem 5.6 we have that $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Case $\ell = 3$. We will show that $\mathrm{Gal}(K(J[3])/K)$ contains $\mathrm{Sp}_{2g}(\mathbb{F}_3)$ for $K = \mathbb{Q}(\zeta_3)$. By Lemma 5.4 then we have $\mathrm{Gal}(\mathbb{Q}(J[3])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_3)$.

Note that hypothesis $(2\mathrm{G}+\epsilon)$ forces $g \geq 6$. Since $p_t > g \geq 6$, it is unramified in $K/\mathbb{Q}$ and $f(x)$ has type $1-\{2\}$ at all primes dividing p_t. The existence of a transvection in $\mathrm{Gal}(K(J[3])/K)$ is ensured by Lemma 2.9.

Let $\mathfrak{p}_2, \mathfrak{p}_3$ be primes of K above p_2 and p_3 respectively. By hypothesis (3), p_2 and p_3 split in K, so $\#\mathbb{F}_{\mathfrak{p}_2} = p_2$ and $\#\mathbb{F}_{\mathfrak{p}_3} = p_3$, and $f(x)$ has type $1-\{q_1, q_2\}$ at $\mathfrak{p}_2$ and type $2-\{q_3\}$ at $\mathfrak{p}_3$. Let us remark that $p_2, p_3, q_1, q_2, q_3 \neq 3$ since $q_4 < q_1 \leq q_2 < q_3$ and $p_2, p_3 > g \geq 6$. By Lemma 3.2, the G_K-module $J[3]$ is absolutely irreducible.

The hyperelliptic curve C/K is semistable at all primes $\mathfrak{p} \nmid p_2, p_2', p_3, p_3'$ by hypothesis (ss). As p_2, p_2', p_3, p_3' are unramified in $K/\mathbb{Q}$, $f(x)$ has the same type above these primes in K as over $\mathbb{Q}$. In particular $f(x)$ is admissible at all primes by Lemmas 4.9, 4.10 and 4.11. By hypothesis (TT), J has totally toric reduction at $\lambda \mid 3$ and so, by Proposition 4.14 $J[3]$ is 3-admissible at λ. By Proposition 4.7 $J[\ell]$ is strongly quasi-unramified. By Proposition 4.4 $J[3] \otimes \overline{\mathbb{F}}_3$ is primitive.

Theorem 5.3 shows that $\mathrm{Sp}_{2g}(\mathbb{F}_3) \subseteq \mathrm{Gal}(K(J[3])/K)$, as required.

Case $\ell = 2$. Recall[4] that $\mathbb{Q}(J[2])$ is the splitting field of $f(x)$. We just need to ensure that the Galois group of $f(x)$ is the full symmetric group S_{2g+2}.

Hypothesis (S_{2g+2}) guarantees the existence of primes p_{irr} and p_{lin} such that $f(x)$ modulo p_{irr} is irreducible, and $f(x)$ modulo p_{lin} factors as an irreducible polynomial times a linear factor. These factorisations ensure the existence of a $2g+2$ cycle and a $2g+1$ cycle in the Galois group of $f(x)$.

By hypothesis (2T), the inertia group at p_t acts as a transposition on the roots of $f(x)$.

Since using $2g+2$ and $2g+1$ cycles it is possible to conjugate a transposition to any other transposition, and the symmetric group is generated by transpositions, we deduce that the Galois group of the splitting field of $f(x)$ is S_{2g+2}, as required. □

Remark 6.6. Hypothesis $(2\mathrm{G}+\epsilon)$ does not hold for $g = 0, 1, 2, 3, 4, 5, 7$ and 13, but we expect it to hold for all other g, and have numerically verified it for $g \leq 10^7$.

For this exceptional list of small genera our method still makes it possible to find hyperelliptic curves with $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for all but a small set of primes ℓ (see Theorem 6.2, Remark 6.3, hypothesis (S_{2g+2}) and the proofs of cases $\ell = 2, 3$ of Theorem 6.5):

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$.

[4]As in [Cor01], $J[2]$ is generated by divisors $D_i = (t_i, 0) - (t_1, 0)$ for $i = 2, \ldots, 2g+2$ subject to the unique relation $\sum_i D_i = 0$, where the t_i are the roots of $f(x)$. Clearly $\mathbb{Q}(J[2])$ is contained in the splitting field of $f(x)$. Conversely, it is easy to see that if $\deg(f) > 4$ and $\sigma \in \mathrm{Gal}(f)$ satisfies $\sigma(D_i) = D_i$ for all i then σ is trivial.

7. Congruence conditions

7.1. **Main theorem: explicit curves.**

The main result of this section is the following explicit version of Theorem 6.5:

Theorem 7.1. *Let g be a positive integer such that there exist primes q_1, q_2, q_3, q_4, q_5 with $2g+2 = q_1+q_2 = q_4+q_5$ and $q_4 < q_1 \le q_2 < q_5 < q_3 < 2g+2$. Let*

$$f_0(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be a polynomial such that

- $a_0 \equiv 2^{2g} \bmod 2^{2g+2}$ *and* $a_i \equiv 0 \bmod 2^{2g+2-i}$ *for all* $i > 0$*;*
- $f_0(x)$ *has type* $1-\{2\}$ *at distinct primes* $p_t, p_t' > g$*;*
- $f_0(x)$ *has* g *distinct double roots in* $\overline{\mathbb{F}}_\ell$ *for every odd prime* $\ell \le g$*;*
- $f_0(x)$ *has type* $1-\{q_1,q_2\}$ *at a prime* $p_2 > 2g+2$*, which is a primitive root modulo* q_1, q_2 *and* q_3*, and* $p_2 \equiv 1 \bmod 3$*;*
- $f_0(x)$ *has type* $2-\{q_3\}$ *at a prime* $p_3 > 2g+2$*, which is a primitive root modulo* q_3*, and* $p_3 \equiv 1 \bmod 3$*;*
- $f_0(x)$ *has type* $1-\{q_4,q_5\}$ *at a prime* $p_2' > 2g+2$*, which is a primitive root modulo* q_3, q_4 *and* q_5*;*
- $f_0(x)$ *has type* $2-\{q_5\}$ *at a prime* $p_3' > 2g+2$*, which is a primitive root modulo* q_5*;*
- $f_0(x)$ *modulo a prime* p_{irr} *is irreducible;*
- $f_0(x)$ *modulo a prime* p_{lin} *factors as an irreducible polynomial times a linear factor.*

Let $C : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$ with $f(x) \in \mathbb{Z}[x]$ monic and squarefree such that

(1) $f(x) \equiv f_0 \bmod N$*, where*

$$N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^2 \cdot p_2'^2 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{\substack{3 \le p \le g \\ prime}} p^2,$$

(2) $f(x)$ *mod* p *has no roots of multiplicity greater than* 2 *in* $\overline{\mathbb{F}}_p$ *for all primes* p *not dividing* N*.*

Then

$$\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \text{ for all primes } \ell \neq 2, \\ S_{2g+2} \text{ for } \ell = 2, \end{cases}$$

where $J = \mathrm{Jac}(C)$*.*

Proof. Clearly hypothesis $(2\mathrm{G}+\epsilon)$ of Theorem 6.5 is satisfied.

Since $f(x) \equiv f_0 \bmod N$ then by Lemma 7.4 $f(x) \in \mathbb{Z}[x]$ satisfies hypotheses (2T), (p_2), (p_3), (p_2') and (p_3') of Theorem 6.5.

Hypotheses (TT) and (ss) are satisfied too by Lemma 7.5, Corollary 7.6 and Lemma 7.7 (ii).

Hypothesis (3) holds since $p_2, p_3 \equiv 1 \bmod 3$.

The existence of p_{irr} and p_{lin} guarantees that (S_{2g+2}) is satisfied.

Therefore by Theorem 6.5 we have that $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ for all odd primes and $\mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q}) \cong S_{2g+2}$. □

Remark 7.2. Condition (2) can be made explicit, in the sense that one can construct examples for (2) in a systematic way as follows.

Recall that $f(x) \bmod p$ has a root of multiplicity greater than 2 if and only if $f, f', f'' \bmod p$ have a common root in $\overline{\mathbb{F}}_p$. To construct a suitable polynomial, first pick any $f(x)$ satisfying (1) and such that $f(x) \bmod p$ has no roots of multiplicity greater than 2 for all primes $p < 2g$ not dividing N. Let

$$\tilde{N} = N \cdot \prod_{\substack{p < 2g,\ p \nmid N \\ \text{prime}}} p.$$

By changing the linear term of $f(x)$ by a multiple of $\tilde{N}$, ensure that $f'(x)$ and $f''(x)$ have no common roots in $\overline{\mathbb{Q}}$, so that for some polynomials $a(x), b(x) \in \mathbb{Z}[x]$ we have $a(x)f'(x) + b(x)f''(x) = M \in \mathbb{Z} \setminus \{0\}$. This guarantees that $f(x) \bmod p$ does not have roots of multiplicity greater than 2 for all primes $p \nmid M$.

If $p \mid M$ with $p \nmid \tilde{N}$ then there exists $c \in \mathbb{F}_p$ such that $f(x) + c \bmod p$ is non-zero at the $\overline{\mathbb{F}}_p$-roots of $f''(x)$, as $p > 2g = \deg f''$. Thus, by the Chinese Remainder Theorem, there exist $z \in \mathbb{Z}$ such that $f(x) + z\tilde{N} \bmod p$ is non-zero at the $\overline{\mathbb{F}}_p$-roots of $f''(x)$ for every $p \mid M$ with $p \nmid \tilde{N}$. Hence, $f(x) + z\tilde{N}$ satisfies conditions (1) and (2) as required.

We now turn to the proof of the congruence conditions used in the proof of Theorem 7.1. For the remainder of this section F will be a local field of odd residue characteristic p. Let $C : y^2 = f(x)$ be a hyperelliptic curve over F with $f(x) \in \mathcal{O}_F[x]$ monic and squarefree and let $J = \mathrm{Jac}(C)$.

7.2. Congruences and type $t - \{q_1, \dots, q_k\}$.

The description of polynomials of type $t - \{q_1, \dots, q_k\}$ in terms of congruences follows from the following version of Hensel's lemma for lifting factorisations (see [Bou85, III.4.3, Théorème 1]):

Theorem 7.3 (Hensel's Lemma for lifting factorisations)**.** *Let F be a local field and let $f(x) \in \mathcal{O}_F[x]$ be a monic polynomial. Let $m \geq 1$ and suppose that*

$$f(x) \equiv \prod_{0 \leq i \leq k} g_i(x) \bmod \pi_F^m,$$

where $g_i(x) \in \mathcal{O}_F[x]$ are monic polynomials such that for every $i \neq j$ the roots of $\overline{g}_i(x)$ are distinct from the roots of $\overline{g}_j(x)$. Then there exist unique monic polynomials $\tilde{g}_0(x), \dots, \tilde{g}_k(x) \in \mathcal{O}_F[x]$ such that $\tilde{g}_i(x) \equiv g_i(x) \bmod \pi_F^m$ and

$$f(x) = \prod_{0 \leq i \leq k} \tilde{g}_i(x).$$

Lemma 7.4. *Let $f_0(x), f(x) \in \mathcal{O}_F[x]$ be monic polynomials. If $f_0(x)$ has type $t - \{q_1, \dots, q_k\}$ and*

$$f(x) \equiv f_0(x) \bmod \pi_F^{t+1},$$

then $f(x)$ has type $t - \{q_1, \dots, q_k\}$.

Proof. The result follows from Theorem 7.3 with $m = t + 1$ by Definition 1.3 and Definition 1.2. □

7.3. **Semistability at odd primes.**

Lemma 7.5. *Suppose p is an odd prime and $f(x) \in \mathcal{O}_F[x]$ is a monic polynomial.*

(i) If all roots of $\overline{f}(x)$ in $\overline{\mathbb{F}}_p$ have multiplicity at most 2, then J is semistable. Moreover, if there are d roots of multiplicity 2, then J has toric dimension $\min(d, g)$.

(ii) If $\overline{f}(x)$ is separable or $f(x) \in \mathcal{O}_F[x]$ has type $t-\{2, 2, \ldots, 2\}$, where the number of twos is between 1 and $g+1$, then J is semistable.

Proof. Clearly *(ii)* follows from *(i)*.

For simplicity we will use the results and notation of Section 2.1 to prove *(i)*.

Let R be the set of roots of $f(x)$, with $\alpha_1, \alpha_1', \ldots, \alpha_d, \alpha_d'$ the roots that reduce to double roots in $\overline{\mathbb{F}}_p$, i.e. $\overline{\alpha}_i = \overline{\alpha}_i'$. The clusters are singleton roots, the set R and $\mathfrak{s}_i = \{\alpha_i, \alpha_i'\}$ for $i = 1, \ldots, d$. We readily compute

$$d_R = 0, \qquad \mu_R = \lambda_R = 0, \qquad \epsilon_R = \gamma_R = \mathbf{1}, \qquad \text{and so } \ V_R = \mathbf{1}^{\oplus(2g-2d)};$$

and

$$I_{\mathfrak{s}_i} = I_F, \qquad \mu_{\mathfrak{s}_i} = 0, \qquad \lambda_{\mathfrak{s}_i} = d_{\mathfrak{s}_i} \in \frac{1}{2}\mathbb{Z}, \qquad \epsilon_{\mathfrak{s}_i} = \mathbf{1},$$

$$\gamma_{\mathfrak{s}_i} = \begin{cases} \mathbf{1} & \text{if } \lambda_{\mathfrak{s}_i} \in \mathbb{Z}, \\ \text{order two} & \text{if } \lambda_{\mathfrak{s}_i} \notin \mathbb{Z}, \end{cases} \qquad \text{and so } \ V_{\mathfrak{s}_i} = 0.$$

It follows from Theorem 2.3 that

$$H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell) = \begin{cases} \mathbf{1}^{\oplus(2g-2d)} \oplus (\mathbf{1}^{\oplus d} \otimes \mathrm{Sp}(2)) & \text{if } d < g+1, \\ \mathbf{1}^{\oplus g} \otimes \mathrm{Sp}(2) & \text{if } d = g+1; \end{cases}$$

where ℓ is any prime $\ell \neq p$. In particular, inertia acts unipotently on $H^1_{\acute{e}t}(C/\overline{F}, \mathbb{Q}_\ell)$, so J is semistable (see [GR72, Proposition 3.5]) and has toric dimension $\min(d, g)$. □

Corollary 7.6. *Let p be an odd prime and suppose that $\overline{f}(x)$ has g double roots over $\overline{\mathbb{F}}_p$. Then J is semistable and has totally toric reduction.*

7.4. **Good reduction at $p = 2$.**

Lemma 7.7. *Let F be a finite extension of $\mathbb{Q}_2$ and let*

$$f(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_1 x + a_0 \in F[x].$$

If either

(i) $a_0 - \frac{1}{4} \in \mathcal{O}_F, a_{2g+1} \in \mathcal{O}_F^\times$ and $a_i \in \mathcal{O}_F$ for $1 \leq i \leq 2g$, or

(ii) $a_0 \equiv 2^{2g} \bmod 2^{2g+2}, a_{2g+1} \equiv 2 \bmod 4$ and $a_i \equiv 0 \bmod 2^{2g+2-i}$ for $1 \leq i \leq 2g$,

then C has good reduction. In particular I_F acts trivially on $J[\ell]$ for every odd prime ℓ.

Proof. (ii) The substitution $x = 2X$, $y = 2^{g+1}Y$ shows that (i) implies (ii).

(i) The substitution $y = Y + \frac{1}{2}$ transforms the model of C into

$$Y^2 + Y = f(x) - \frac{1}{4} \in \mathcal{O}_F[x].$$

All points on this affine chart are smooth since the partial derivative with respect to Y is nowhere vanishing. The substitution $V = 1/x, W = Y/x^{g+1}$ gives the chart at infinity $W^2 + WV^{g+1} = V^{2g+2}(f(1/V) - \frac{1}{4})$. There is a unique point at infinity,

corresponding to $V = 0$, which is a smooth point since the partial derivative with respect to V is a unit: the linear term of the RHS is $a_{2g+1}V$. Therefore, the curve has good reduction at 2.

The last statement then follows from the theorem of Néron-Ogg-Shafarevich. □

8. An example

In this section we construct an explicit hyperelliptic curve of genus 6 with maximal mod ℓ Galois representation for all primes ℓ, following the recipe of Theorem 7.1.

First of all, $2g+2 = 14 = 7+7 = 3+11$, so we can take $q_1 = q_2 = 7$, $q_4 = 3$, $q_5 = 11$ and $q_3 = 13$. Now pick primes that satisfy the appropriate congruence conditions:

$$p_t = 7,\ p_t' = 11,\ p_{lin} = 23,\ p_{irr} = 29,\ p_2 = 19,\ p_2' = 41,\ p_3 = 37,\ p_3' = 17.$$

For example p_2 is a primitive root modulo 7 and 13 and it is congruent to 1 modulo 3, so the choice $p_2 = 19$ meets the requirements of Theorem 7.1, and similarly for the other primes.

The theorem then gives the following requirements for

$$f_0(x) = x^{14} + a_{13}x^{13} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]:$$

$f_0(x)$ has type $1-\{2\}$ at 7, $f_0(x)$ has type $1-\{2\}$ at 11,
$f_0(x)$ has type $1-\{7,7\}$ at 19, $f_0(x)$ has type $1-\{3,11\}$ at 41,
$f_0(x)$ has type $2-\{13\}$ at 37, $f_0(x)$ has type $2-\{11\}$ at 17,
$f_0(x)$ is irreducible mod 23, $f_0(x)$ factors as linear $\cdot$ irreducible mod 29,
$f_0(x)$ has 6 distinct double roots over $\overline{\mathbb{F}}_3$ and $\overline{\mathbb{F}}_5$,
$a_0 \equiv 2^{12} \bmod 2^{14}$, $a_{13} \equiv 2 \bmod 4$ and $a_i \equiv 0 \bmod 2^{14-i}$ for $1 \le i \le 12$.

By Definition 1.3, Lemma 7.4 and Corollary 7.6, it is enough to have:

$$\begin{aligned}
f_0(x) &\equiv (x^{12}+2x^8+5x^7+3x^6+2x^5+4x^4+5x^2+3)\cdot(x^2-7) && \bmod 7^2,\\
f_0(x) &\equiv (x^{12}+x^8+x^7+4x^6+2x^5+5x^4+5x^3+6x^2+5x+2)\cdot(x^2-11) && \bmod 11^2,\\
f_0(x) &\equiv (x^7-19)\cdot((x-1)^7-19) && \bmod 19^2,\\
f_0(x) &\equiv (x^{11}-41)\cdot((x-1)^3-41) && \bmod 41^2,\\
f_0(x) &\equiv (x^{13}-37^2)\cdot(x+1) && \bmod 37^3,\\
f_0(x) &\equiv (x^{11}-17^2)\cdot(x^3+x+14) && \bmod 17^3,\\
f_0(x) &\equiv x^{14}+x^8+5x^7+16x^6+x^5+18x^4+19x^3+x^2+22x+5 && \bmod 23,\\
f_0(x) &\equiv (x+1)\cdot(x^{13}+7x+27) && \bmod 29,\\
f_0(x) &\equiv (x-1)\cdot x\cdot(x^6+2x^4+x^2+2x+2)^2 && \bmod 3^2,\\
f_0(x) &\equiv (x-1)\cdot x\cdot(x^6+x^4+4x^3+x^2+2)^2 && \bmod 5^2,\\
f_0(x) &\equiv x^{14}+2x^{13}+2^{12} && \bmod 2^{14}.
\end{aligned}$$

By the Chinese Remainder Theorem on the coefficients we obtain the following polynomial for $f_0(x)$:

$$\begin{aligned}
f_0(x) = x^{14} &+ 112297655051805859275993907 4\,x^{13} + \\
&+ 1120184609916242124087443456\,x^{11} + \\
&+ 16859902456993495593000140 80\,x^9 + \\
&+ 14228269579836355474178703 36\,x^7 + \\
&+ 607434202225985243206107136\,x^5 + \\
&+ 533014336994715937945092096\,x^3 + \\
&+ 127684591382595558689905049 6\,x + \\
&+ 1024732349070635834864435 2\,x^{12} + \\
&+ 1863982903647860009218867 20\,x^{10} + \\
&+ 3875299526726535859354992 64\,x^8 + \\
&+ 5859839986254299973080350 72\,x^6 + \\
&+ 1820210247550502007557029888\,x^4 + \\
&+ 5958034051549429458797527 04\,x^2 + \\
&+ 1323672381818030813822668800.
\end{aligned}$$

The reduction modulo p of the polynomial $f_0(x)$ has no roots of multiplicity greater than 2 for any prime $p \notin \{19, 41, 37, 17\}$, so by Theorem 7.1 the Jacobian J_0 of

$$C_0 : y^2 = f_0(x)$$

has

$$\mathrm{Gal}(\mathbb{Q}(J_0[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{12}(\mathbb{F}_\ell) \text{ for all primes } \ell \neq 2, \\ S_{14} \text{ for } \ell = 2. \end{cases}$$

Moreover, setting

$$N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^2 \cdot p_2'^2 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot 3^2 \cdot 5^2 = 22015907575118164360654848 00,$$

the same conclusion holds for any curve $C : y^2 = f(x)$ with $f(x) \equiv f_0(x) \bmod N$ such that $f(x) \bmod p$ has no roots of multiplicity greater than 2 for all primes $p \notin \{19, 41, 37, 17\}$.

References

[AAK+15] Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. Galois representations and galois groups over $\mathbb{Q}$. In *Women in Numbers Europe: Research Directions in Number Theory*, pages 191–205. Springer International, Cham, 2015.

[AAK+16] Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. Large Galois images for Jacobian varieties of genus 3 curves. *Acta Arith.*, 174(4):339–366, 2016.

[ADW16] Sara Arias-de-Reyna, Luis Dieulefait, and Gabor Wiese. Classification of subgroups of symplectic groups over finite fields containing a transvection. *Dem. Math.*, 49(2):129–148, May 2016.

[AK13] Sara Arias-de-Reyna and Christian Kappen. Abelian varieties over number fields, tame ramification and big Galois image. *Math. Res. Lett.*, 20(1):1–17, 2013.

[ALS16] Samuele Anni, Pedro Lemos, and Samir Siksek. Residual representations of semistable principally polarized abelian varieties. *Res. Number Theory*, 2:Art. 1, 12, 2016.

[AS15] Samuele Anni and Samir Siksek. On Serre's uniformity conjecture for semistable elliptic curves over totally real fields. *Math. Z.*, 281(1-2):193–199, 2015.

[AV11] Sara Arias-de-Reyna and Núria Vila. Galois representations and the tame inverse Galois problem. In *WIN—Women in Numbers*, volume 60 of *Fields Inst. Commun.*, pages 277–288. Amer. Math. Soc., Providence, RI, 2011.

[Bou85] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1985. Algèbre commutative. Chapitres 1 à 4. [Commutative algebra. Chapters 1–4], Reprint.

[BSW16] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. Squarefree values of polynomial discriminants i. *ArXiv e-prints*, nov 2016. `https://arxiv.org/abs/1611.09806`.

[Cor01] Gunther Cornelissen. Two-torsion in the jacobian of hyperelliptic curves over finite fields. *Archiv der Mathematik*, 77(3):241–246, 2001.

[DD09] Tim Dokchitser and Vladimir Dokchitser. Regulator constants and the parity conjecture. *Invent. Math.*, 178(1):23, 2009.

[DDMM18] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan. Arithmetic of hyperelliptic curves over local fields. *ArXiv e-prints*, aug 2018. `https://arxiv.org/abs/1808.02936`.

[Die02] Luis Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[GR72] Alexander Grothendieck and Michel Raynaud. *Modeles de Néron et monodromie*, pages 313–523. Springer Berlin Heidelberg, Berlin, Heidelberg, 1972.

[Hal08] Chris Hall. Big symplectic or orthogonal monodromy modulo l. *Duke Math. J.*, 141(1):179–203, 2008.

[Hal11] Chris Hall. An open-image theorem for a general class of abelian varieties. *Bull. Lond. Math. Soc.*, 43(4):703–711, 2011. With an appendix by Emmanuel Kowalski.

[Lom15] Davide Lombardo. Explicit open image theorems for some abelian varieties with trivial endomorphism ring. *ArXiv e-prints*, August 2015. https://arxiv.org/abs/1508.01293.

[LSTX19] Aaron Landesman, Ashvin Swaminathan, James Tao, and Yujie Xu. Surjectivity of Galois representations in rational families of abelian varieties. *Algebra Number Theory*, 13(5):995–1038, 2019.

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mil86] James Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[Pap13] Mihran Papikian. Non-archimedean uniformization and monodromy pairing. *Contemp. Math.*, pages 123–160, 2013.

[Ray74] Michel Raynaud. Schémas en groupes de type $(p, \dots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[SZ05] Alice Silverberg and Yuri Zarhin. Inertia groups and abelian surfaces. *J. Number Theory*, 110(1):178–198, 2005.

[Zar79] Yuri Zarhin. Abelian varieties, l-adic representations and Lie algebras. Rank independence on l. *Invent. Math.*, 55(2):165–176, 1979.

[Zar10] Yuri Zarhin. Hyperelliptic Jacobians and Steinberg representations. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 217–225. Soc. Math. France, Paris, 2010.

[Zyw15] David Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. *ArXiv e-prints*, August 2015. https://arxiv.org/abs/1508.07655.

Aix-Marseille Université, CNRS, Centrale Marseille, Institut de Mathématiques de Marseille, Case 907, 163, avenue de Luminy, F13288 Marseille cedex 9, France

Email address: samuele.anni@gmail.com

Department of Mathematics, King's College London, Strand, London, WC2R 2LS, United Kingdom

Email address: vladimir.dokchitser@kcl.ac.uk